clarify the Examiner's comment in the Advisory Action of February 14, 2001. Moreover, the Response to Arguments appears to overlook the primary arguments of Applicants, to wit, the Office Action states "in essence, Applicants have been arguing that the key pairs are provided to a multi-client manager unit, instead of by a multi-client manager unit to an undisclosed recipient as the claim actually states". Applicants have not made such an argument and respectfully request a showing as to where this interpretation finds its root. Moreover, it is unclear which claim the Examiner is referring to.

Since the Examiner appears to recite the exact rejections from the previous Office Action, Applicants respectfully reassert the remarks made in the Response to the previous Office Action. In addition, Applicants wish to attempt to clarify their position in an effort to persuade the Patent Office that the claims are allowable in view of the cited references.

With respect to Claim 1, the Final Office Action states that the claim is not allowable because it "would have been obvious to a person of ordinary skill in the art at the time the invention was made to give users the ability to define the validity period for certificates, as taught by Ellison, in the public key update system of Lewis." As previous noted, the Lewis reference is directed to a completely different problem and hence a solution from Applicants' claimed invention. The Lewis reference is directed to selecting replacement keys so that it is computationally difficult to determine a replacement key from its masked version. An active public key and a hash of a replacement key is provided by a key server to nodes of the network. Each time a key request is performed, the active public key is discarded. A key replacement message is signed by an active private key and a replacement private key. Accordingly, the message is signed by a replacement private key from an entity that knows the replacement private key before the message is sent.

The cited portion of Ellison, is not enabling and hence cannot be used to render the claim obvious (see, e.g., Rockwell Intern. Corp. v. U.S., 147 F.3d 1358, 1365 (Fed.Cir. 1998). In any event, to the extent understood, as stated by the Examiner, Ellison mentions quite generally that a user may decide that they want a two day validity period for carrying out a transaction so that a user may define how long the validity period may be. Ellison is completely silent as to how this may be done. More importantly, Applicants claim a distinctly different approach and actually

Ellison appears to teach away from Applicants' claimed invention. As stated by the Examiner, if Ellison generally teaches to give users the ability to define the validity period for certificates, Applicants respectfully submit that the claimed invention prevents users from defining such a validity period. This is because Applicants claim, among other things, that certification authority referred to as a multi-client trust authority, and not a user, provides selectable digital signature expiry data including at least public verification key expiry data and selectable private signing key expiry data that are selected on a per-client basis wherein the digital signature key pairs are not shared among users and digitally storing both selective public key expiry data and selected private key expiry data for association with a new digital signature key pair for a client. Accordingly, "users" do not select their own validity periods as allegedly taught by Ellison. The system taught by Ellison, wherein a user has the ability to define the validity period for a certificate, would effectively override the entire trust relationship of the system since the user would be effectively acting as its own trust authority. In contrast, Applicants claim a multi-client trust authority that services multiple clients which provides the selectable validity periods to, for example, a central operator. Accordingly, even if the Examiner's position is to be accepted, the resulting system as taught by Ellison operates in a completely different manner and does not include, among other things, a centralized certification authority or multi-client trust authority that provides the methods or operation as claimed. In addition, as noted above, Ellison does not describe how to make or otherwise carry out the idea expressed by Ellison. The dependent claims help in part further to define Applicants' way of providing the unique approach as claimed.

The dependent claims add additional subject matter not taught or suggested by the cited references. For example, Claim 3 requires the step of providing variable update privilege control on a per client basis to the multi-client manager unit to facilitate denial of updating the digital signature key pair on a per client basis. The Office Action cites Col. 7, ll. 64-65 of the Lewis reference. However, Applicants are unable to find any mention of providing variable update privilege control on a per client basis so that the multi-client manager unit cannot deny the updating of a digital signature key pair. Applicants respectfully request a showing as to such a teaching. In fact, the cited section appears merely to say that the key replacement message is broadcast having certain fields. Accordingly, this claim is also believed to be in condition for allowance.

As to Claim 6, the Office Action alleges that such a step is inherent to Ellison and that an interface to select validity periods is required. Applicants respectfully challenge such a position since Ellison is completely silent as to how a user would select a validity period. Moreover, from the teachings of Ellison it appears that if, for example, a user had a two-day period that this period would likely be for all certificates. As such, no interface is required. However, the Office Action appears to mischaracterize the claimed invention since the claim requires providing a user interface to facilitate setting of the selectable expiry data to a desired state wherein the interface referred to in Claim 6 is that associated with the multi-client manager unit. In fact, for argument's sake, even if a user interface to set a selectable expiry data to a desired state was inherent in Ellison, which Applicants submit it is not, the user interface would be available to a user as taught by Ellison which again would allow the user to set the date where Applicants claim an opposite approach, namely having the multi-client manager unit or trust authority have the ability to provide the selectable expiry data. As such, a centralized control of expiry data for multiple users is provided in contrast to the teachings of Ellison. Accordingly, Applicants respectfully submit that this claim is also in condition for allowance.

Claims 5, 19 and 25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Lewis and Ellison as applied to Claims 1, 14 and 21 and further in view of Applicants' admitted prior art. Applicants respectfully reassert the remarks made in the previous Response to Office Action.

Claim 7 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Lewis and Ellison as applied to Claim 1. Applicants respectfully reassert the remarks made above with respect to Claim 1 and also respectfully submit that Lewis does not teach or suggest, among other things, generating, by the multi-client manager unit, the new digital signature key pair for a client in response to the multi-client manager unit receiving a digital signal signature key pair update request. Applicants respectfully request a showing of such a teaching.

Accordingly, Applicant respectfully submits that the amended claims are in condition for allowance. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a conference would expedite the prosecution of the instant application.

Respectfully submitted,

By:________________________
Christopher J. Reckamp
Registration No. 34,414

Date: September 4, 2001

VEDDER, PRICE, KAUFMAN &
KAMMHOLZ
222 N. LaSalle Street
Chicago, IL 60601
(312) 609-7500; FAX: (312) 609-5005